KUSANO 16F022
I.D.S. (3)

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-066836
(43)Date of publication of application : 05.03.2003

(51)Int.Cl. G09C 1/00
G06F 17/60

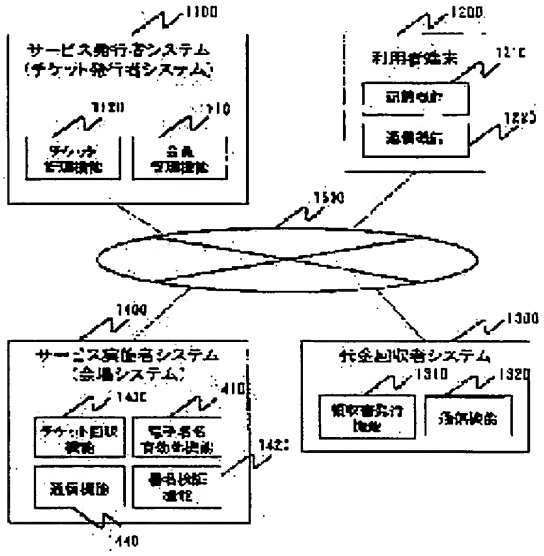
(21)Application number : 2001-257129
(22)Date of filing : 28.08.2001

(71)Applicant : HITACHI LTD
(72)Inventor : NOYAMA HIDEO
MATSUKI TAKESHI
TERADA SHUJI
KOJIMA TAKESHI
IWAMURA MITSURU

(54) ELECTRONIC SIGNATURE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To solve the problem that a means for easily correcting an electronic document even when the status of dealings is changed is not available and an electronic ticket needs to be issued at a center or by using a storage medium after the dealings are completed.
SOLUTION: A service issuer system 1100 generates an electronic signature for the ticket by using a secret key, ciphers the electronic signature by using a password, and provides the ticket and electronic signature for a user terminal 1200 and an open key for a service executor system 1400; when a charge collector system 1300 collects the charge for the ticket, the password is obtained from the service issuer system 1100 and provided for the user terminal 1200, the service executor system 1400 obtains the ticket, electronic signature, and password from the user terminal 1200, deciphers the electronic signature with the password, and applies the open key to the deciphered electronic signature to verify the adequacy of the ticket.

図 1



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－66836
（Ｐ２００３－６６８３６Ａ）
(43)公開日　平成15年３月５日(2003.3.5)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
G09C 1/00	640	G09C 1/00	640	B 5J104
			640	D
G06F 17/60	140	G06F 17/60	140	
	240		240	
	410		410	A

審査請求　未請求　請求項の数15　ＯＬ　（全12頁）　最終頁に続く

(21)出願番号　特願2001－257129(Ｐ2001－257129)

(22)出願日　平成13年８月28日(2001.8.28)

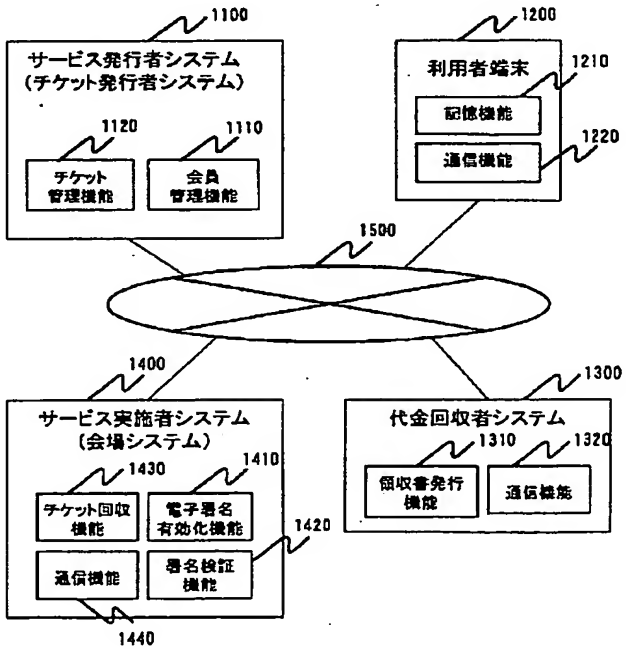
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　野山　英郎
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　松木　武
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報サービス事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】電子署名方法

(57)【要約】
【課題】従来、取引のステータスが変更されても電子文書を簡単に修正する手段がなく、電子チケットなどを発行するにはセンタで取引完了後に発行するか記憶媒体を使わなければならなかった。
【解決手段】サービス発行者システム1100が、秘密鍵を用いてチケットの電子署名を生成し、パスワードによって電子署名を暗号化し、チケットと電子署名を利用者端末1200へ提供し、公開鍵をサービス実施者システム1400へ提供し、代金回収者システム1300が、チケットに対する代金を回収した場合に、サービス発行者システム1100からパスワードを取得し、利用者端末1200へ提供し、サービス実施者システム1400が、利用者端末1200からチケットと電子署名とパスワードを取得し、パスワードによって電子署名を復号化し、復号化された電子署名に公開鍵を作用させてチケットの正当性を検証する。

図１



1　　2

【特許請求の範囲】

【請求項１】電子文書に電子署名を施すための、コンピュータによる電子署名方法において、
共通鍵生成手段が、前記電子文書を利用する利用者が所定の条件を満たした場合に前記利用者へ発行されるための共通鍵を生成し、
秘密鍵生成手段が、前記電子署名を得るための秘密鍵と、前記秘密鍵に対応し、前記電子文書の正当性を検証するための公開鍵とを生成し、
電子署名生成手段が、前記秘密鍵を前記電子文書に作用させることによって、前記電子文書の電子署名を生成し、
暗号化演算手段が、前記共通鍵によって前記電子署名を暗号化し、
前記電子文書と前記暗号化された電子署名は、前記電子文書に前記電子署名を施す電子署名者から、前記利用者へ発行され、
前記公開鍵は、前記電子署名者から、前記電子文書の正当性を検証する検証者へ発行される電子書名方法。

【請求項２】前記所定の条件は、前記利用者が前記電子文書に対する対価の支払いを完了したことを含む請求項１に記載の電子署名方法。

【請求項３】電子文書管理手段が、前記利用者へ発行された前記電子文書について、前記電子文書に対する対価の支払いの有無を管理する請求項２に記載の電子署名方法。

【請求項４】共通鍵発行手段は、代金を回収する代金回収者から前記対価の支払完了の通知を受けた場合に、前記代金回収者の代金回収者へ、前記共通鍵を発行し、
前記共通鍵は、前記代金回収者から、前記利用者へ発行される請求項２に記載の電子署名方法。

【請求項５】ハッシュ値生成手段が、前記電子文書にハッシュ関数を作用させることによって、ハッシュ値を生成し、
前記電子署名は、前記ハッシュ値の電子署名である請求項１に記載の電子署名方法。

【請求項６】前記電子文書は、電子チケット又は電子クーポンを含む請求項１に記載の電子署名方法。

【請求項７】電子文書に電子署名を施すための電子署名システムにおいて、
前記電子文書を利用する利用者が所定の条件を満たした場合に、前記利用者へ発行されるための共通鍵を生成する共通鍵生成手段と、
前記電子署名を得るための秘密鍵と、前記秘密鍵に対応し、前記電子文書の正当性を検証するための公開鍵とを生成する秘密鍵生成手段と、
前記秘密鍵を前記電子文書に作用させることによって、前記電子文書の電子署名を生成する電子署名生成手段と、
前記共通鍵によって前記電子署名を暗号化する暗号化演算手段とを備え、
前記電子文書と前記暗号化された電子署名は、前記利用者へ発行され、
前記公開鍵は、前記電子文書の正当性を検証する検証者へ発行される電子書名システム。

【請求項８】電子署名によって電子文書の正当性を検証するための、コンピュータによる電子文書検証方法において、
記憶手段が、前記電子文書に前記電子署名を施す電子署名者によって発行された公開鍵を記憶し、
第１の取得手段が、前記電子署名者から前記電子文書の利用者へ発行された共通鍵を取得し、
第２の取得手段が、前記利用者の利用者端末から、前記電子文書と、前記共通鍵によって暗号化された電子署名とを取得し、
復号化演算手段が、前記共通鍵によって、前記電子署名を復号化し、
検証手段が、前記電子署名に前記公開鍵を作用させることによって、前記電子文書の正当性を検証する電子文書検証方法。

【請求項９】前記検証手段が、前記電子署名の生成に利用されたハッシュ関数を前記電子文書に作用させることによってハッシュ値を得、前記公開鍵によって前記復号化された電子署名を復号化し、前記ハッシュ値と前記公開鍵によって復号化された電子署名の値とを比較することによって、前記電子文書の正当性を検証する請求項８に記載の電子文書検証方法。

【請求項１０】利用許可手段が、前記電子文書が正当であることが検証された場合に、前記電子文書の利用を許可する請求項９に記載の電子文書検証方法。

【請求項１１】電子署名によって電子文書の正当性を検証するための電子文書検証システムにおいて、
前記電子文書に前記電子署名を施す電子署名者によって発行された公開鍵を記憶する記憶手段と、
前記電子署名者から前記電子文書の利用者へ発行された共通鍵を取得する第１の取得手段と、
前記利用者の利用者端末から、前記電子文書と、前記共通鍵によって暗号化された電子署名とを取得する第２の取得手段と、
前記共通鍵によって、前記電子署名を復号化する復号化演算手段と、
前記電子署名に前記公開鍵を作用させることによって、前記電子文書の正当性を検証する検証手段とを備えた電子文書検証システム。

【請求項１２】電子署名が施された電子文書の利用者から、前記電子文書に対する対価を回収するための、コンピュータによる代金回収方法において、
通知手段が、前記利用者から前記対価を回収した場合に、前記対価を回収した旨を、前記電子文書を発行した発行者へ通知し、

取得手段が、前記電子署名の暗号化に利用された共通鍵を、前記発行者から取得し、
前記共通鍵は、前記対価を回収した代金回収者から前記利用者へ発行される代金回収方法。
【請求項１３】電子署名が施された電子文書の利用者から、前記電子文書に対する対価を回収するための代金回収システムにおいて、
前記利用者から前記対価を回収した場合に、前記対価を回収した旨を、前記電子文書を発行した発行者へ通知する通知手段と、
前記電子署名の暗号化に利用された共通鍵を、前記発行者から取得する取得手段とを備え、
前記共通鍵は、前記対価を回収した代金回収者から前記利用者へ発行される代金回収システム。
【請求項１４】電子署名が施された電子文書の利用者から、前記電子文書に対する対価を回収するための、コンピュータによる代金回収方法において、
第１の取得手段が、前記利用者の利用者端末から、前記電子署名を取得し、
通知手段が、前記利用者から前記対価を回収した場合に、前記対価を回収した旨を、前記電子文書を発行した発行者へ通知し、
第２の取得手段が、前記電子署名の暗号化に利用された共通鍵を、前記発行者から取得し、
復号演算手段が、前記共通鍵によって前記電子署名を復号化し、
発行手段が、復号化された電子署名を、前記利用者端末へ発行する代金回収方法。
【請求項１５】電子署名が施された電子文書の利用者から、前記電子文書に対する対価を回収するための代金回収システムにおいて、
前記利用者の利用者端末から、前記電子署名を取得する第１の取得手段と、
前記利用者から前記対価を回収した場合に、前記対価を回収した旨を、前記電子文書を発行した発行者へ通知する通知手段と、
前記電子署名の暗号化に利用された共通鍵を、前記発行者から取得する第２の取得手段と、
前記共通鍵によって前記電子署名を復号化する復号演算手段と、
復号化された電子署名を、前記利用者端末へ発行する発行手段とを備えた代金回収システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、公開鍵暗号を用いた電子署名方法及びその電子署名方法を用いた電子チケットシステムに係り、特に取引ステータスによってデジタル署名の有効性を遷移させるための電子署名方法に関する。
【０００２】
【従来の技術】従来の技術として、特開平11-261550号公報には、電子文書から特徴を抽出して特徴データを生成し、この特徴データを当事者の暗号鍵で暗号化して暗号化データを作成し、さらにこの暗号化データに日付などの外部認証データを付与し、これを外部認証者の暗号鍵で暗号化することにより、当事者であっても文書の改竄ができないようにすることで、文書の電子化を推進するものが開示されている。
【０００３】また、特開2000-315265号公報には、ICカードの読取り・書き込みが可能な情報処理端末と、決済サービスを行なうサービスセンタの情報処理装置との通信において、情報処理端末は、発券指示が入力されるとICカードに対応した電子チケット発券可否をチェックし、発券指示に応じた支払処理依頼を決済サービスセンタに送信し、支払処理結果通知を受信すると、ICカードに発券を指示し、ICカードは発券を指示されると電子チケットを発券して格納するものが開示されている。
【０００４】
【発明が解決しようとする課題】特開平11-261550号公報によると、電子文書に、外部認証者の暗号鍵を作用させることにより、電子文書を作成した本人であっても文書の改竄ができないようにすることができる。言い換えると、電子文書に何らかの変更をする為には、本人の復号鍵と外部認証者の復号鍵の両方が必要になる。例えば、貸借契約書の電子文書を保存するには有効であるが、支払いが行なわれた場合でも、この電子文書を「支払い済み」と変更することはできない。なぜなら、電子文書の一部であっても変更ができた場合、この電子文書がオリジナルの貸借契約書と同じ内容であるとは、誰も保証できなくなるからである。
【０００５】特開2000-315265号公報によると、ICカードというセキュアデバイスを用いることで、チケットの券種の選択、支払手続き、発券と受取のプロセスを個人所有端末で行なうことができ、受取った「チケット」を、サービス提供される駅などでそのまま利用することができるようになる。しかし、サービスセンタの情報処理装置と接続して決済サービスを受けるためには、クレジットカード会社等の金融機関に対して決済サービスの申し込みをし、専用のICカードを入手しておく必要がある。そして、金融機関の決済サービスは誰でも受けられる訳ではなく、未成年や定職に就いていない人は加入できない場合があった。
【０００６】本発明の第１の目的は、代金の支払い等により、ある時点以降において電子文書のステータスが変更したとしても、その有効性を保証できる仕組みを提供し、電子文書の有効性を簡単な方法で遷移させる（変更する）ことが可能な電子署名方法を提供することである。
【０００７】本発明の第2の目的は、金融機関やサービスプロバイダが提供する決済サービスに加入していない

人であってもサービスを受けられるようにすることである。即ち、ICカード等の特別の媒体を用いずに、チケットの電子化が可能な方法を提供することによって、利用者が販売店の営業時間や配達に要する期間に影響されずに、いつでもチケットを購入できるようにすることであり、誰もがこのような電子チケットサービスを享受できるようにすることである。

【０００８】

【課題を解決するための手段】本発明は、電子署名者システムが、電子文書（例えば、電子チケットや電子クーポン等）と共通鍵（例えば、パスワード）と秘密鍵とその秘密鍵に対応する公開鍵とを生成し、秘密鍵を電子文書に作用させることによって電子署名を生成し、共通鍵によって電子署名を暗号化し、電子文書と暗号化された電子署名を利用者端末へ提供し、検証者システムへ公開鍵を提供し、代金回収者システムが、電子文書に対する対価の支払いを受けた場合に、その旨を電子署名者システムへ通知し、電子署名者システムから共通鍵を取得し、共通鍵を利用者端末へ提供し、検証者システムが、利用者端末から電子文書と暗号化された電子署名と共通鍵を取得し、共通鍵によって暗号化された電子署名を復号化し、復号化された電子署名に公開鍵を作用させることによって電子文書の正当性を検証する。尚、検証者システムの代わりに、代金回収者システム又は利用者端末が、共通鍵によって電子署名を復号化してもよい。共通鍵によって電子署名が復号化されると、電子署名が有効となる。即ち、電子署名のステータスが無効から有効へ変化する。

【０００９】

【発明の実施の形態】以下、本発明の実施例を詳細に説明する。

【００１０】図１は、本発明の全体システム概要を示す説明図であり、関与者及び各関与者が持つ機能概要を示している。

【００１１】本発明における関与者は、サービスを受けるための権利情報を発行するサービス発行者と、サービスを提供するサービス実施者と、サービスに対する代金を回収する代金回収者と、サービスを利用する利用者である。例えば、コンサートのチケットや旅行クーポンチケットでは、チケットの販売を専門にするチケット業者や旅行代理店が存在する。本発明は、このような販売代行業者が既に存在する業種において特に有効と考えられる。なぜなら、サービス実施者がこのような販売代行業者を使うのは、その販売チャネルを利用して多くの消費者との接点を持ちたいからであり、さらに代金回収を行なう手段が必要だからである。尚、代金回収者がいない場合は、サービス発行者又はサービス実施者が代金の回収を行う。

【００１２】以下、コンサートチケットを例にして説明する。

【００１３】サービス発行者はチケットを発行し販売する業者(以下、チケット発行者とする)であり、サービス実施者はコンサートを運営する会社であり、コンサート会場でチケットを回収する。利用者は、チケット発行者からチケットを購入し、サービス実施者へそのチケットを譲渡し、コンサートを聴く者である。

【００１４】サービス発行者システム1100は、利用者を管理する為の会員管理機能1110、及び、チケットを管理する為のチケット管理機能1120を、少なくとも持っている。会員管理機能1110は、利用者から利用者の個人情報（例えば、氏名、住所、電話番号、電子メールアドレス等）を取得し、利用者ごとに利用者を特定するための会員ＩＤ（例えば、会員番号や会員パスワード等の文字や数字の組み合せ）を、利用者へ発行する。サービス発行者システム1100は、利用者の個人情報と会員ＩＤとを対応づけて記憶する。チケット管理機能1120は、チケットが保証しているサービス等の内容、及びチケットの販売ステータス(例えば、販売前、予約済、未決済、決済済、未使用、使用済等)を管理する。なお、チケットを管理するためのデータテーブルに関しては、図4に後述する。また、サービス発行者システム1100は、鍵生成手段を持ち、電子署名を生成するための秘密鍵と、秘密鍵に対応し、チケットの正当性を検証するための公開鍵を生成する。

【００１５】利用者端末1200は、サーバにアクセスして該サーバのコンテンツをダウンロードする為の通信機能1220と、ダウンロードしたデータを保存する為の記憶機能1210を持っており、サービス発行者システムから入手した電子チケットデータ(以下、電子チケットと略す)等を保存することができる。なお、本発明における電子チケットは、チケットが保証しているサービス内容及びチケットの販売ステータスを遷移させる、即ち、電子署名を有効化する機能を有する電子署名が含まれている。

【００１６】代金回収者システム1300は、利用者端末1200から電子的な請求書データを読み取り、この請求書に基づいて支払い（決済）が行なわれた場合は、電子的な領収書を発行する為の領収書発行機能1310と、この取引内容をサービス発行者システム1100に通知するための通信機能1320を持つ。なお、この領収書に相当する電子的なデータとして、本発明ではパスワードを使用する。このパスワードは、チケット発行者によって決定されるのが好ましい。このパスワードは、暗号化及び復号化が可能な共通鍵の役割を果たす。つまり、サービス発行者システム1100は、パスワード生成機能を持ち、電子署名を暗号化及び復号化（有効化）するためのパスワードを生成する。

【００１７】サービス実施者システム1400は、利用者端末1200から電子チケットとパスワード（領収書）を読み取り、電子チケットにパスワード（電子的な領収書のデータ列）を作用させて電子署名を有効化する処理を行な

う電子署名有効化機能1410と、有効化された電子署名を用いてチケットの正当性を検証する為の署名検証機能1420と、チケットを回収して保管する為のチケット回収機能1430と、精査処理をする為に回収したチケットをサービス発行者に送るための通信機能1440を持っている。そして、サービス発行者システム1100は、精査処理を行なって、チケットのステータスを使用済みに遷移させる。

【００１８】ネットワーク1500は、インターネットや電話回線、無線通信網などのいずれのネットワーク、あるいはそれらの組み合せでも良く、ネットワークの種類や規模に限定されるものではない。

【００１９】図２は、電子チケットを発行する際の処理概要を示すフロー図である。

【００２０】初めに、利用者端末1200は、サービス発行者システム1100に対して、ステップ2100でチケットの申込みを行なう。具体的には、利用者端末1200は、利用者からチケットの種類や枚数の入力、及び利用者を特定するための会員ＩＤ等の入力を受け、該情報をサービス発行者システム1100へ送信する。

【００２１】次に、サービス発行者システム1100は、利用者の認証を行う。具体的には、利用者端末1200から取得した会員ＩＤが、サービス発行者システム1100内に予め登録されている会員情報の会員ＩＤにうち、一致するものがあるか否かを判断する。入力情報及び入手情報が、事前に登録されている会員情報と一致したならば正規の会員と判断し、ステップ2220に処理を移す。尚、サービス発行者システム1100は、利用者（会員）をより確実に認証するために、会員ＩＤに加え、利用者端末1200の固有ID（例えば、電話番号や端末ＩＤ等）を入手し、サービス発行者システム1100内に予め登録されている会員情報と比較して会員の認証を行なってもよい。利用者端末1200の固有IDは、利用者端末1200のメーカや利用者が加入する通信キャリア（例えば、電話会社等）によって、利用者端末1200ごと付与され、利用者端末1200の記憶領域に記憶される。利用者端末1200のメーカや通信キャリアは、利用者の個人情報と利用者端末1200の固有IDとを対応づけて管理している。

【００２２】ステップ2220では、電子チケットの作成を行なう機能である。具体的には、電子チケットの元になるデータを作成し、該データを暗号化する。なお、電子チケットの作成アルゴリズム（暗号化や電子署名の処理を含む）は図３に後述する。つぎに、該暗号化データをコード画像に変換する。そして、ステップ2240において、サービス発行者システム1100内に会員毎に個別に設けられたディレクトリを作成し、このディレクトリに該コード画像を保存する。そして、該ディレクトリと画像ファイル名を足し合わせたURL（Uniform Resource Locator）を利用者端末1200に返信する。URLは、電子チケットの保存場所を特定するための情報である。

【００２３】ここで、電子チケットが、バーコードや２次元コードで表現されていれば、以降で述べる代金回収者システム1300やサービス実施者システム1400で、汎用的な読取装置（例えば、バーコードリーダ、２次元コードリーダ等）を使うことができる。但し、利用者端末1200と読取装置のインタフェースが一致していれば、これらのデータ受渡は可能であり、電子チケットがバーコードや２次元コードに限定されるものではない。

【００２４】利用者端末1200は、利用者の指示に応じて、URLを用いて、URLによって特定されたディレクトリにアクセスし、そのディレクトリから電子チケットをダウンロードする。ステップ2120において、利用者端末1200の記憶機能1210は、利用者から保存場所の入力を受付け、指定されたローカルな記録領域に電子チケットを格納する。尚、利用者端末1200がURLを用いて電子チケットをダウンロードする替わりに、サービス発行者システム1100が、利用者端末1200へ直接に電子チケットを送信してもよい。

【００２５】また、サービス発行者システム1100は、ステップ2140において、前記URLの情報を電子メールに記載すると共に、会員ＩＤをキーとしてサービス発行者システム1100内の会員情報を特定しその会員情報からから利用者のメールアドレスを抽出し、ＵＲＬが記載された電子メールを抽出されたメールアドレスへ送信するのが好ましい。この処理は、本発明の本質では無いが、例えば無線通信を用いてこの取引が行なわれる場合、周囲の環境変化によってダウンロードの途中に通信が遮断される可能性が無いとは言えず、正常にダウンロードが行われなかった時のバックアップ機能は必須になる。図３は、ステップ2220における電子チケットの作成機能を詳細に説明したフローチャートである。

【００２６】電子チケット作成機能１(3000)は、ステップ3100のチケットデータ生成手段において、申込みされたチケットの値0(3110)を作成する。例えば、コンサートのチケットであれば、コンサート及びアーチストの名称、開催日時、コンサート会場の名称、席種や座席番号、価格等がこの値0に含まれる。ステップ3200において、値0を署名対象として、サービス発行システム1100内に記憶されたハッシュ関数を用いて、値0のハッシュ値を作成する。尚、ハッシュ関数とは、文字列に数値（ハッシュ値）を対応させるための適当な関数をいう。次に、ステップ3300において、該ハッシュ値にチケット発行者の秘密鍵3310を作用させ、署名データを生成する。即ち、秘密鍵3310によってハッシュ値を暗号化する。この暗号化データが署名データとなる。尚、署名を行うための秘密鍵と、署名を検証するための公開鍵とは対になっている。サービス発行者システム1100は、秘密鍵3310と共に公開鍵3200を生成し、公開鍵3200を代金回収者システム1300及びサービス実施者システム1400へ送信する。そして、ステップ3400において、パスワード3410を鍵として署名データを暗号化し、ステップ3400にお

いて、この暗号値と値0(3110)を結合して値1(3510)を作成する。パスワード3410は、電子チケットの申し込みごとに設定されてもよいし、利用者ごとに（会員ＩＤ）に設定されてもよい。

【００２７】図４は、サービス発行者システム1100のチケット管理機能1120において管理するデータテーブル4000と、図３で生成された電子チケット（値１）との関係について示す説明図である。

【００２８】データテーブル4000は、チケットを識別するためのチケットIDを格納するためのフィールド4110と、チケットの内容（コンサート及びアーチストの名称、開催日時、コンサート会場の名称、席種や座席番号、価格等）を示すチケットデータを格納するためのフィールド4120と、パスワード3410を格納するためのフィールド4130と、取引ステータスを格納するためのフィールド4140等で構成されている。取引ステータスとは、チケットの販売が開始されてから、使用後に回収されるまでの間において、その時点におけるチケットの状態を示すものであり、例えば、(販売前、予約済、未決済、決済済、未使用、使用済等のステータスがある。また、このデータテーブル4000は、当然のことながら、電子チケット4200や電子請求書4300、電子領収書4400と連携しており、これらはチケットID（4110，4210，4310，4410）で結び付けられている。従って、チケットデータには、データテーブル4000のチケットデータと同じ内容が記載されている。同様に、署名データには、データテーブル4000の取引ステータスと同じ内容が記載される。そして、署名データの取引ステータスが変更されたときは、データテーブル4000の取引ステータスも可能な限り早いタイミングで更新されるのが好ましい。

【００２９】一方、請求書データ4320には、金額及び有効期限及び支払可能な場所が記載されている。また、後述するが、請求書データ4320は取引ステータスを変更する為の鍵を含む場合もある。署名データ4330は、前述の請求書データ4320に対する電子署名であり、電子チケットに含まれる署名データ4230とは異なるものである。また、領収書データ4420は、データテーブル4000のパスワードと、代金回収者システム1300の店舗識別番号を含んでいる。署名データ4430は、領収書データ4420に対する電子署名であり、代金回収者システム1300の秘密鍵を使って署名する。

【００３０】図５は、図２における利用者端末1200がダウンロードに失敗した場合に、この利用者端末1200を救済するための処理について示したフロー図である。

【００３１】利用者端末1200がサービス発行者システム1100との一連のトランザクションにおいてネットワーク障害等によってダウンロードに失敗したとしても、サービス発行者システム1100から発行された発行確認の電子メールを受信することが可能である。したがって、利用者端末1200がこの電子メールを受信することができれば、ステップ5100において、この電子メールに記載されたURL情報を利用者端末1200のブラウザに渡すことで、会員専用のディレクトリに再度接続することができる。

【００３２】サービス発行者システム1100は、ステップ5200において、接続を要求してきた利用者端末1200からその利用者端末1200の固有IDを入手し、この固有IDが事前に登録された会員情報と一致するかどうかを検証する。この利用者端末の認証が成功した場合（利用者端末1200から取得した固有IDと、サービス発行者システム1100内に記憶された固有ＩＤとが一致した場合）、アクセス制御機能5220はブラウザのURLを会員専用のディレクトリに遷移させる。そして、利用者端末1200は電子チケットをダウンロードしてローカルな記憶領域に保存する。なお、ステップ5300は前述の図2のステップ2400と同じ処理なので、詳細な説明は省略する。

【００３３】図６は、チケット代金の支払いを実店舗で行なうことを可能とする為のフロー図である。

【００３４】初めに、利用者端末1200は、ステップ6100において、利用者端末のディスプレイ部に電子請求書を表示する。

【００３５】代金回収者システム1300は、ステップ6200において、電子請求書4300を読み込み、署名データ4330と請求書データ4320を取得する。また、代金回収者システム1300は、サービス発行者システム1100から、サービス発行者システム1100の秘密鍵と対の公開鍵を受信する。次に、この請求書データ4320とサービス発行者システム1100の公開鍵を用いて署名データ4330を検証する。この検証が成功した場合、この電子請求書4300は正しいものと判断して、利用者の支払いを受け付ける。

【００３６】そして、代金回収者から支払いが完了の指示を受けた場合、ステップ6220において、パスワード3410を入手する処理を行なう。即ち、サービス発行者システム1100に対して、ステータスの更新依頼及び販売実績の通知を行ない、その代わりにサービス発行者システム1100からパスワード3410を入手する。そして、ステップ6240において、該パスワード3410と代金回収者を特定するための店舗識別番号店舗識別番号を含んだ領収書データを作成する。その結果、代金回収者システム1300は、パスワード3410を取得できるので、このパスワード3410を利用者端末1200に通知することができる。尚、代金回収者システム1300がステータスの更新依頼及び販売実績の通知の代わりにサービス発行者システム1100からパスワード3410を入手する代わりに、電子請求書にパスワード3410を含ませ代金回収者システム1300が利用者端末1200から電子請求書を入手しその電子請求書からパスワードを入手してもよい。利用者端末1200は、ステップ6120において、代金回収者システム1300からパスワード3410と店舗の識別番号を含む領収書データを入手し、利用者端末1200のローカルな記憶領域に保存する。

【００３７】サービス発行者システム1100は、ステップ

6300において、代金回収者システム1300から店舗の販売実績及びステータスの更新依頼を入手し、電子チケットの取引ステータス4140を「予約」から「決済済み」に変更する。尚、サービス発行者システム1100のデータベースに記録されている取引ステータス4140に基づいて、チケット発行者から店舗に対して売上げ請求が行われる。

【００３８】図７は、ステップ2220において電子チケットと同時に作成される電子請求書作成機能を詳細に説明したフローチャートである。

【００３９】代金回収者システム1300は、暗号化するための公開鍵と、その暗号を復号化するための秘密鍵とを予め生成し、その公開鍵をサービス発行者システム1100へ送信する。

【００４０】電子請求書作成機能7000は、ステップ7100において、パスワード3410を暗号対象データとして、代金回収者システム1300の公開鍵で暗号化する。次に、ステップ7200において、この暗号値と請求書データ(金額及び有効期限及び支払可能な場所等)を結合して値2(7210)を作成する。次に、ステップ7300において、値2を署名対象データとして、この署名対象データにハッシュ関数(ダイジェスト関数)を作用させ、ハッシュ値を取得する。さらに、ステップ7400において、このハッシュ値とサービス発行者システム1100の秘密鍵7410を用いて署名データを作成する。そして、署名データ4330と署名対象データ4320を結合して値3（即ち、電子請求書4300）を作成する。

【００４１】図８は、コンサート会場等で電子チケットの検札を行なう処理を示すフロー図である。

【００４２】電子チケットを使う場合、利用者端末1200は、ステップ8100において、利用者端末1200の記憶領域に記憶された１又は複数の電子チケットをディスプレイ部に表示し、利用者から利用を希望する電子チケットの選択を受け、その電子チケットを読み出して、利用者端末1200のディスプレイ部に表示する。また、ステップ8120において、当該電子チケットを有効化する為のパスワード3410、並びに、店舗識別番号をコード画像に変換し、利用者端末1200のディスプレイ部に表示する。

【００４３】サービス実施者システム1400は、ステップ8200において、当該電子チケットを読み取る。また、サービス実施者システム1400は、パスワード3410並びに店舗識別番号の入力を受け付ける。なお、サービス実施者システム1400は、電子チケット及びパスワード3410及び店舗識別番号の入力処理を別々に受け付けても良いし、これらを含む１つのコード画像を利用者端末1200で作成し、このコード画像を一度に受け付けても良い。次に、ステップ8220において、このパスワード3410を用いて電子チケットを複合化する。なお、この複合化処理、並びにチケットの正当性検証処理については、図９において説明する。また、ステップ8240において、正しいチケットと判定されたなら、パスワード3410及び店舗識別番号を回収する。

【００４４】図９は、サービス実施者システム1400において、電子チケットの正当性を検証するための処理を示すフローチャートである。

【００４５】サービス実施者システム1400は、利用者端末1200から電子チケットの値1(3510)を読み込み、ステップ9100において、値0（3110）とその電子署名データに分割する。ただし、この電子署名データは暗号化されており、ステップ9120において、パスワード3410を用いて複合化する。この電子署名データの復号化によって、電子署名データが有効化され、これによって、電子チケットも有効化される。次に、ステップ9140の署名検証手段において、値0（3110）とサービス発行者システム1100の公開鍵3200を用いて、前記復号化した電子署名データの検証を行なう。具体的には、サービス実施者システム1400は、電子署名データの生成に利用されたハッシュ関数を記憶している。そして、サービス実施者システム1400は、値0（3110）にハッシュ関数を作用させ、電子チケットのハッシュ値を得る。一方、サービス実施者システム1400は、パスワードによって復号化された電子署名データを、公開鍵3200を用いて、さらに復号化する。そして、サービス実施者システム1400は、電子チケットのハッシュ値と公開鍵3200を用いて復号化された電子署名データの値とを比較し、両者の値が同一である場合は、電子署名が正当であると判断し、両者の値が同一でない場合は、電子署名が不正であると判断する。ステップ9140において、電子署名が正しいと判断された場合（即ち、署名検証の出力値9160がTRUEである場合）、サービス実施者システム1400は、正しい電子チケットが来たと判断し、会場への入場を許可する旨を表示する。サービス実施者システム1400は、正しい電子チケットが来たと判断し、会場への入場を許可する許可手段（例えば、ゲート）を操作する。尚、サービス実施者システム1400が電子チケットを有効化する代わりに、代金回収者システム1300や利用者端末1200が電子チケットを有効化してもよい。利用者端末1200が電子チケットを有効化するための処理は、代金回収者システム1300やサービス実施者システム1400が電子チケットを有効化するための処理と同様である。

【００４６】なお、サービス実施者システム1400は、ステップ9120において、パスワード3410及び店舗識別番号を回収するが、サービス実施者システム1400にこれらの数値を入力する入力装置を持たっても良い。また、利用者端末1200に表示された数値をサービス実施者システム1400が（文字認識機能を用いて）読み取っても良い。さらに、利用者端末1200がこれらの数値をコード画像に変換しておき、サービス実施者システム1400がこの画像を読み取っても良い。

【００４７】なお、本実施の形態において、サービス発行者システム1100、サービス実施者のシステム1400、代

金回収者システム1300、利用者端末1200は、いわゆるパーソナルコンピュータ、ワークステーション等が用いられ、このようなコンピュータ上で動作するプログラムにより上述した各手段が機能的に実現される。

【００４８】図１１は、本発明を実施する為のハードウェアについて記載した説明図である。

【００４９】サービス発行者システム1100は、チケット及び会員の情報の入力を受ける為のデータ入力装置11010と、電子チケットの保管及びこの領域に対して正しい利用者端末だけにアクセスを許可する為のアクセス制御装置11020と、ネットワーク1500を介して関与者装置にアクセスする為の通信装置11030と、取引の通知及び通信不良をおこした時の連絡手段を提供する為のメール作成装置11040と、電子チケットデータを作成して電子署名を付与し、さらに本発明における署名の無効化を行なう演算装置11050と、テーブル4000においてチケット等を管理する記録装置11060で構成される。

【００５０】また、サービス実施者システム1400は、利用者端末の情報を読み取る為のデータ入力装置11120と、ネットワーク1500を介して関与者装置にアクセスする為の通信装置11130と、電子署名を有効化し、電子署名の検証を行なう為の演算装置11150と、チケットを不正に使わせないようにする為の二重管理装置11140、精査に用いる領収証データを回収保存する為の記録装置11160と、電子署名を検証した結果を表示する為の表示装置11110で構成される。

【００５１】また、特に利用者端末1200は、記憶手段や表示・入力手段や通信手段を持ち、プログラムを搭載できる多機能携帯端末でもよいし、いわゆる携帯電話であっても良いので、いわゆるコンピュータ装置に限定されるものではない。

【００５２】また、代金回収者システム1300は、決済機能及び領収書作成機能を持つことになっているが、請求書の検証や領収書データ（パスワード3410）の発行はサービス発行者システムに持たせることができ、その場合は通信機能のみを持つFAX装置等でも良いので、いわゆるコンピュータ装置に限定されるものではない。

【００５３】以上に述べた実施の形態において、利用者端末がコード画像を作成する為には利用者端末にこの処理プログラムをインストールしていなければならなかったが、Java等の技術を利用し、このプログラムに相当する処理をJavaアプレットとして実装し、該アプレットをサービス発行者システムからダウンロードして利用できれば、インストール作業が不要となり、利用者に特別な負担を強いる必要が無くなる。

【００５４】図１０は、この仕組みをタクシークーポンに適用した場合の関与者と、各関与者の持つ機能について示した説明図である。

【００５５】なお、ここで示すタクシークーポンとは、一般に言うタクシーチケットとは別のものであり、タクシーを利用した時に発行されるクーポン券を集めておき、集めたクーポン券をサービス発行会社に送ると、支払ったタクシー代金の一部がキャッシュバックされるというサービスを実現する為の媒体である。

【００５６】図１における関与者を以下のように置き換える。即ち、サービス発行者はタクシークーポンを発行し管理する業者であり、サービス実施者はタクシークーポンを利用する提携企業であり、代金回収者システムは車載システムであり、利用者端末は社員の携帯端末に相当する。

【００５７】また、タクシークーポン管理会社システム10100が会員管理機能10110及びクーポン管理機能10120を持ち、提携企業システムが電子署名有効化機能10410と署名検証機能10420とクーポン回収機能10430と通信機能10440を持ち、社員の携帯端末10200が記憶機能10210と通信機能10220を持つ。

【００５８】タクシーを利用するとき、社員の携帯端末10200は、タクシークーポン管理会社システム10100にアクセスしてタクシーの予約をする。タクシークーポン管理会社システム10100は、予約を受け付けると、金額の書かれていない請求書とクーポン券を発行し、社員の携帯端末はこれらを入手する。なお、図４における電子チケット4200が当該クーポン券に対応し、電子請求書4300が当該請求書に対応する。

【００５９】一方、車載システム10300が領収書発行機能10310と通信機能10320を持つ。そして、タクシーを利用したとき、車載システム10300は領収書に相当するパスワード3410を発行する。

【００６０】社員が会社に対して旅費の精算要求を行なう場合、提携企業システム10400に対して、電子的なクーポン券とパスワード3410を送信し、クーポン券の正当性が確認された場合は精算要求を受け付け、そうでない場合は受け付けないものとする。

【００６１】以上に述べた実施例は、チケットをクーポン券に置き換えることで、前記電子チケットの実施例と同じ仕組みで実現できる。

【００６２】以上の実施例によると、実店舗において代金の支払いを行ない、これによって電子文書の所有権が移った場合、電子文書の有効性を簡単な方法で遷移させる（変更する）ことが可能になる。即ち、ある時点以降において電子文書の有効性を保証できる電子署名方法を提供することできる。また、チケットの電子化によって、利用者は販売店の営業時間等に影響されず即時にチケットを入手できるというメリットを、誰もが享受できるようにすることができる。即ち、金融機関の提供する決済サービスに加入していない人であっても、このような電子チケットサービスを享受できるようになる。

【００６３】

【発明の効果】本発明によれば、代金の支払い等により、ある時点以降において電子文書のステータスが変更

15　　16

したとしても、その有効性を保証できる仕組みを提供し、電子文書の有効性を簡単な方法で遷移させる（変更する）ことが可能となる。

【００６４】又は、本発明によれば、金融機関やサービスプロバイダが提供する決済サービスに加入していない人であってもサービスを受けられるようになる。

【図面の簡単な説明】

【図１】本発明の全体システム概要を示す説明図であり、関与者及び各関与者が持つ機能概要を示している。

【図２】電子チケットを発行する際の処理概要を示すフロー図である。

【図３】ステップ2220における電子チケットの作成機能を詳細に説明したフローチャートである。

【図４】サービス発行者システム1100のチケット管理機能1120において管理するデータテーブル4000と、図３で生成された電子チケット（値１）との関係について示す説明図である。

【図５】図２における利用者端末がダウンロードに失敗した場合に、この利用者端末を救済するための処理について示したフロー図である。

【図６】チケット代金の支払いを実店舗で行なうことを可能する為の処理を示すフロー図である。

【図７】ステップ2220において電子チケットと同時に作成される電子請求書作成機能を詳細に説明したフローチャートである。

【図８】コンサート会場等で電子チケットの検札を行なう処理を示すフロー図である。

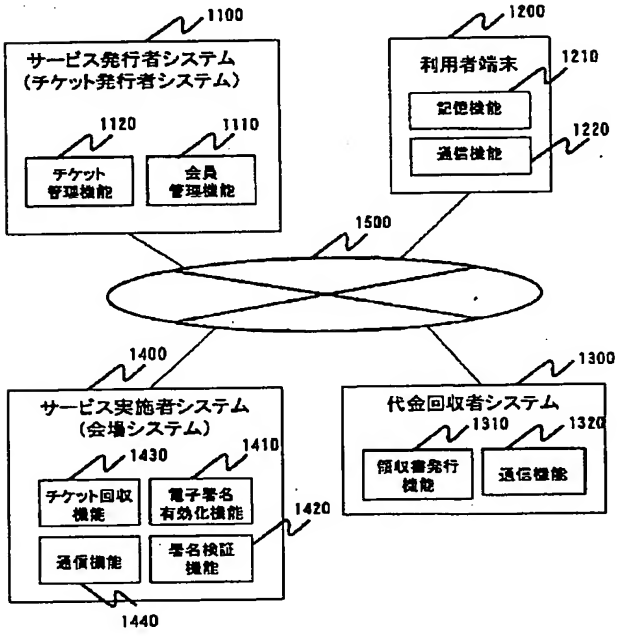
【図９】サービス実施者システム1400において、電子チケットの正当性を検証するための処理を示すフローチャートである。

【図１０】この仕組みをタクシークーポンに適用した場合の関与者と、各関与者の持つ機能について示した説明図である。

【図１１】本発明を実施する為のハードウエア構成に関して記載した説明図である。

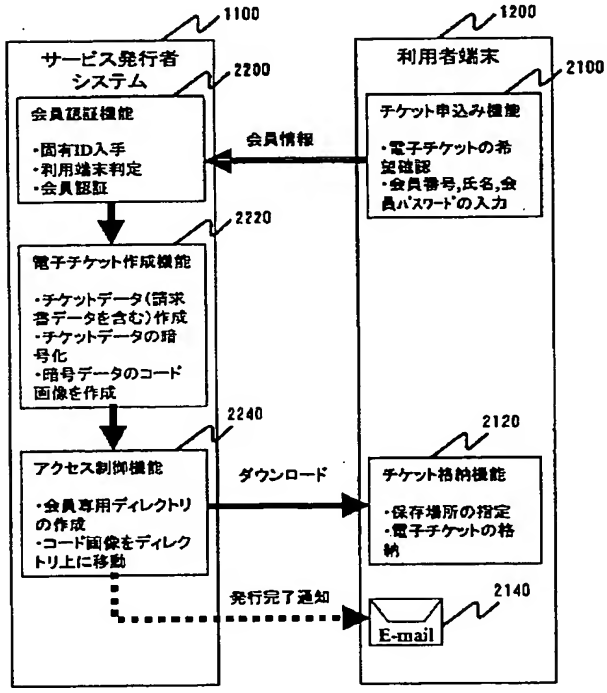
【図１】

図１



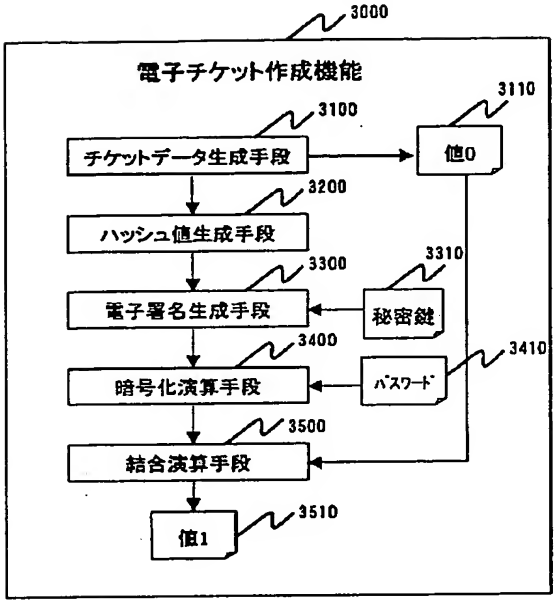
【図２】

図２



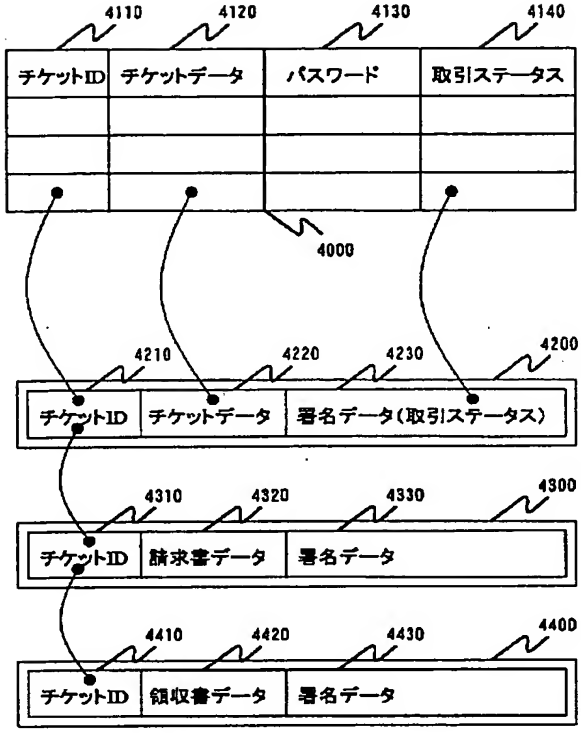
【図３】

図 3



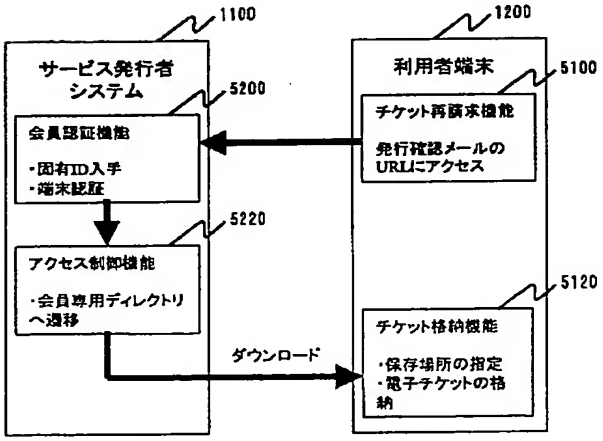
【図４】

図 4



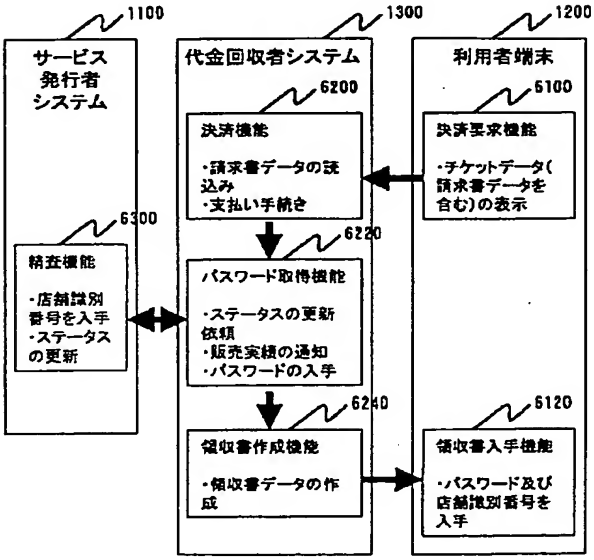
【図５】

図 5



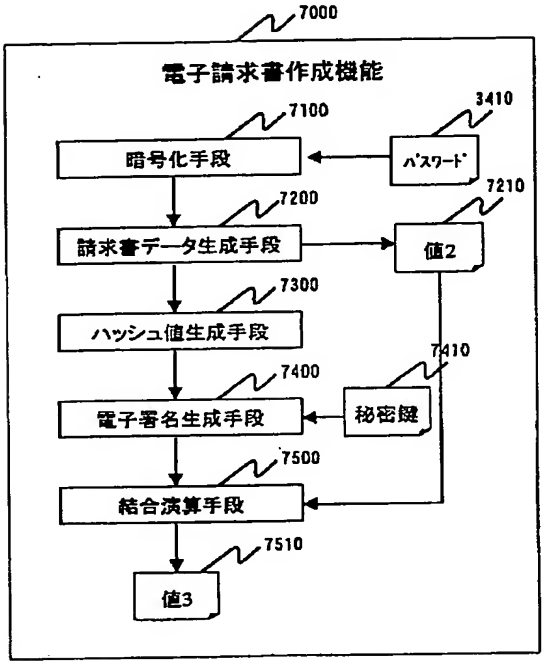
【図６】

図 6



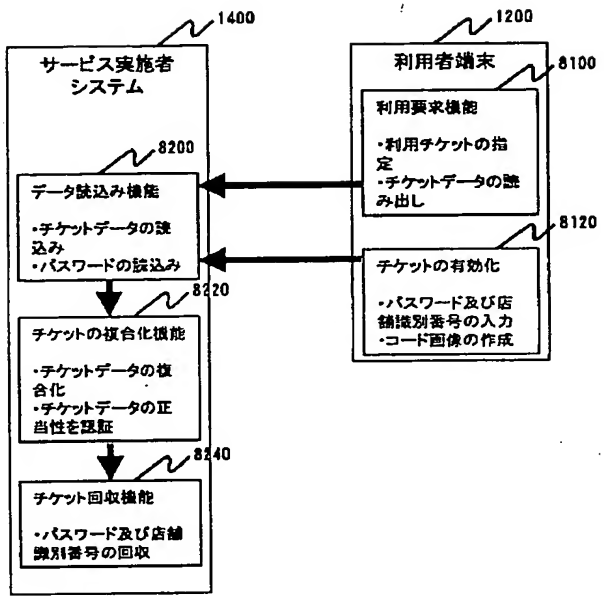
【図７】

図 7



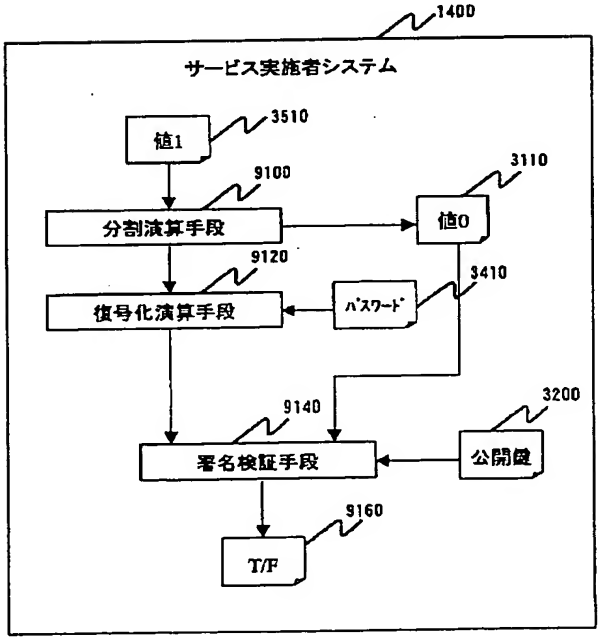
【図８】

図 8



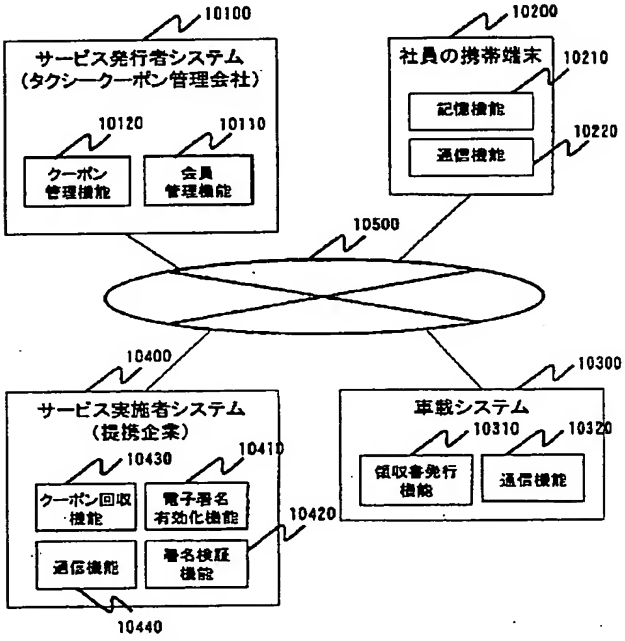
【図９】

図 9



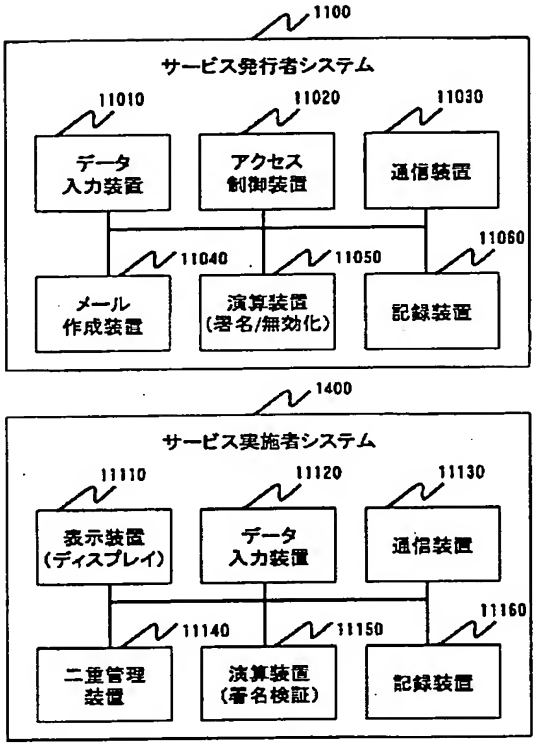
【図１０】

図 10



【図１１】

図 11



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
	424	424	
	512	512	

(72)発明者　寺田　修司
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報サービス事業部内
(72)発明者　小島　岳
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション事業部内
(72)発明者　岩村　充
東京都練馬区中村２－14－17

Ｆターム(参考)　5J104 AA09 LA03 LA05 LA06 NA02
PA10